

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**

## Secure Telematics System Architecture

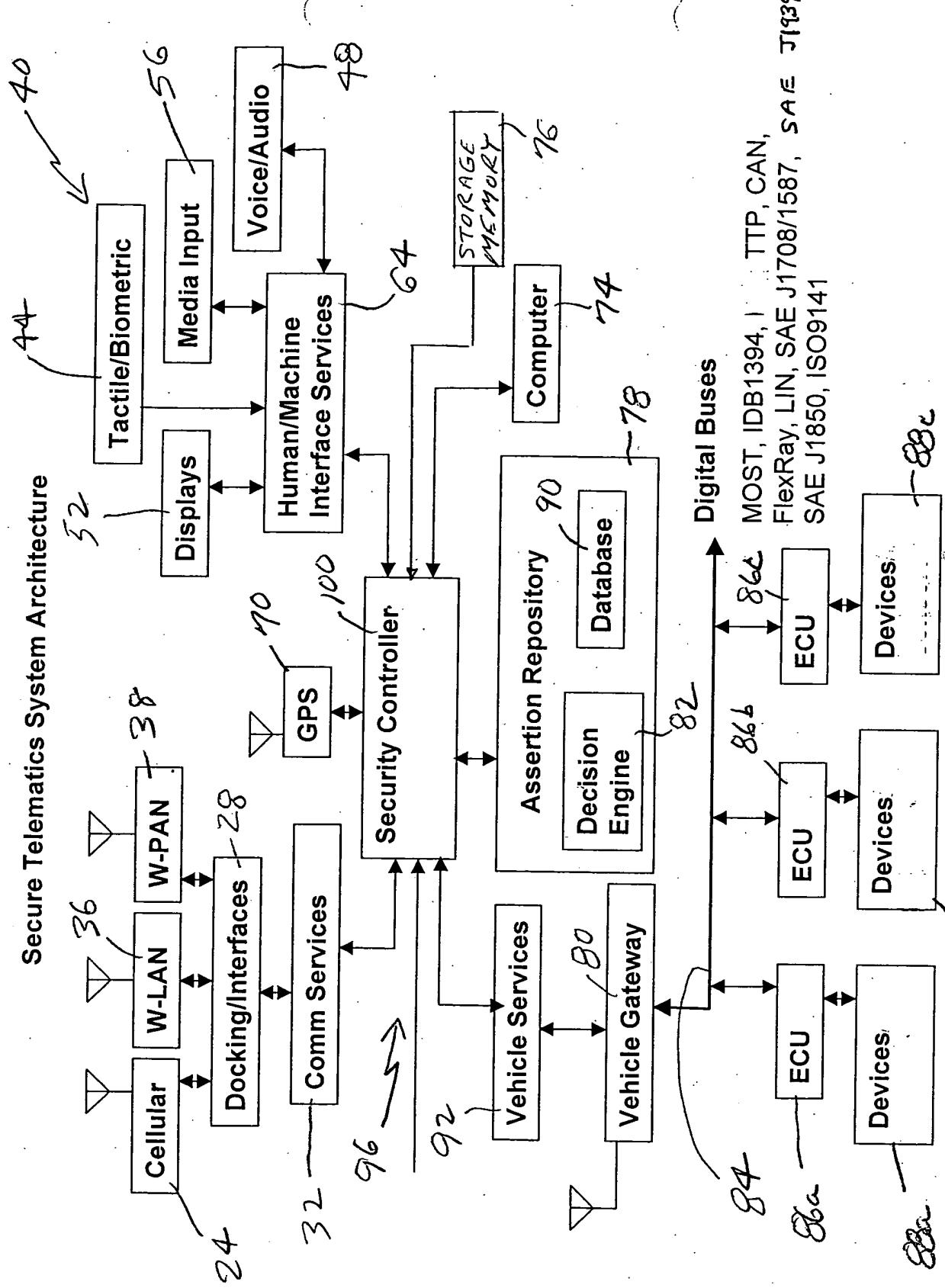


Fig. 1

## Secure Telematics System Architecture 20

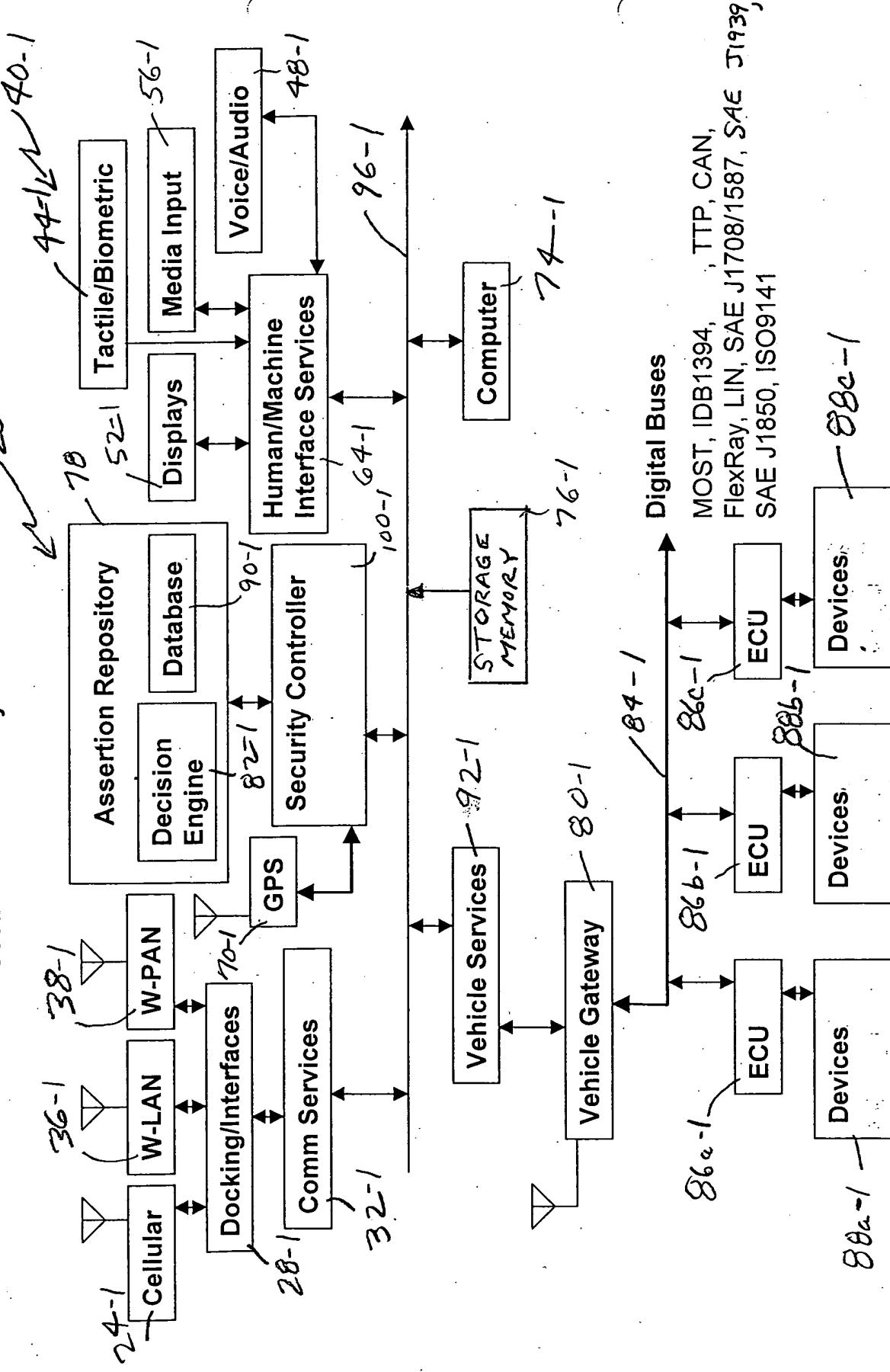


Fig. 2

### KDC-Modeled Security Controller

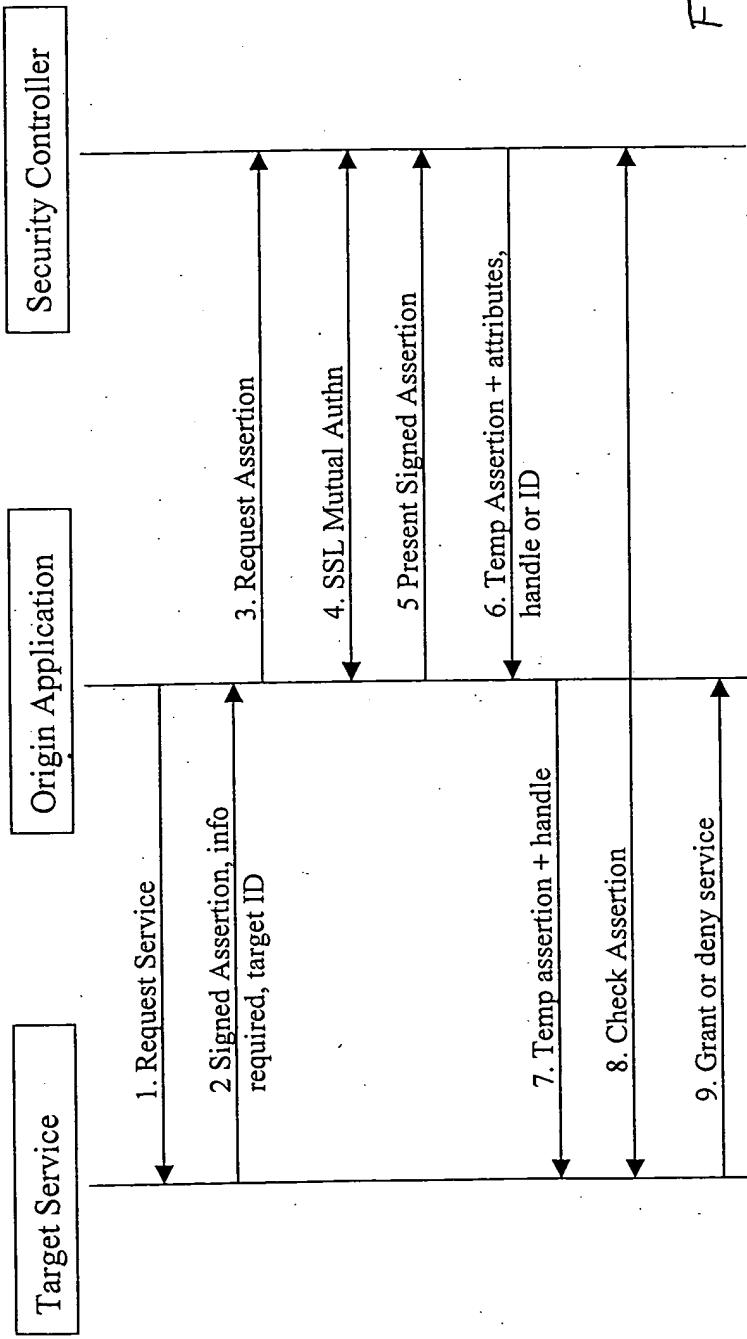


Fig. 3

Flows between the Origin and Target may need to be encrypted to protect against “man-in-the-middle” attacks.

The Origin Application may remain anonymous to the Target Service throughout the transaction.

The assertion check in step 8 could be done against the Security Controller’s PKC, eliminating the need for Target Service to Security Controller communication.

## Anonymous Drive-through Payment

94 "Assertion Repository" ✓ 78

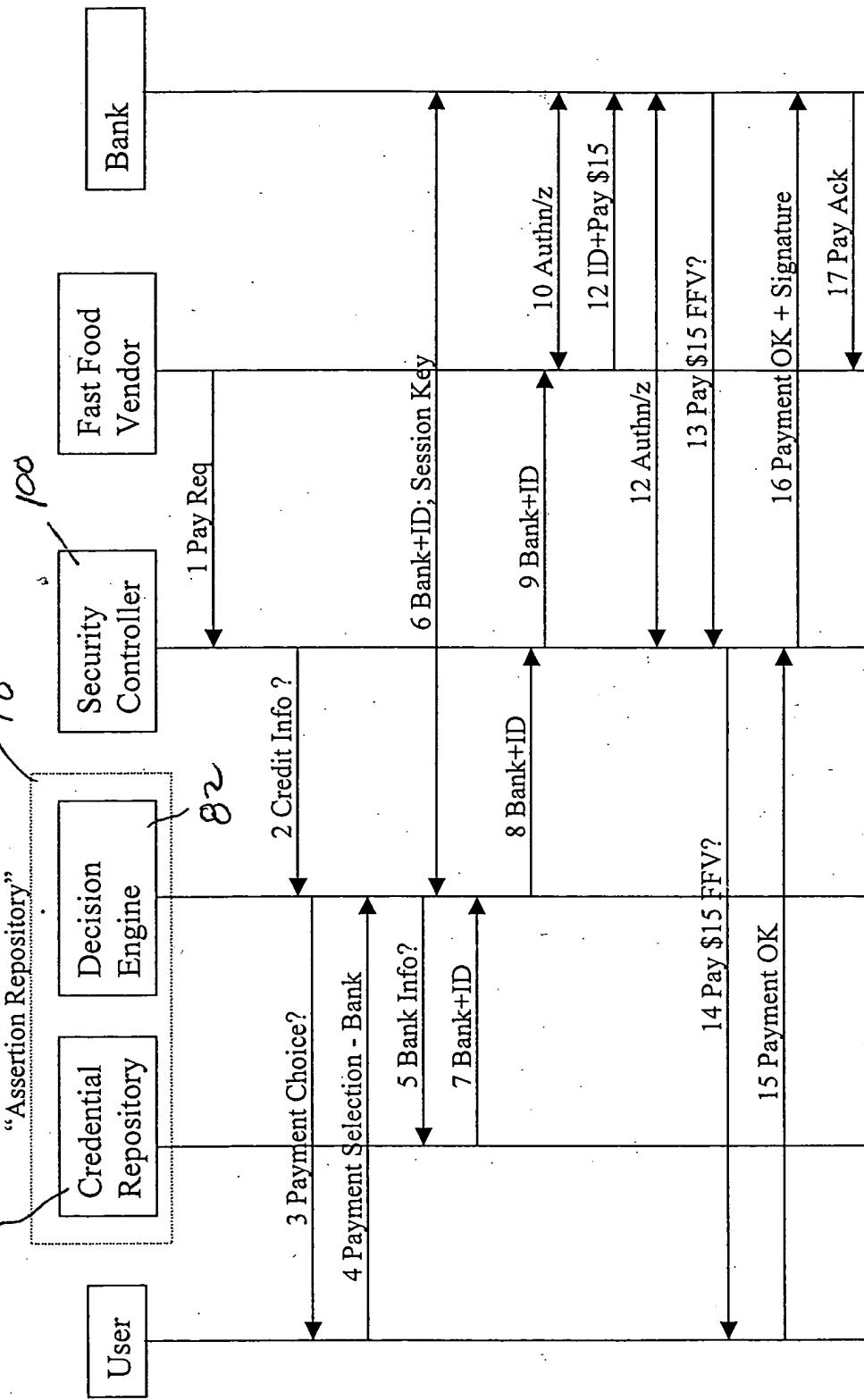


Fig. 4

### Anonymous Toll Payment – Airport Shuttle

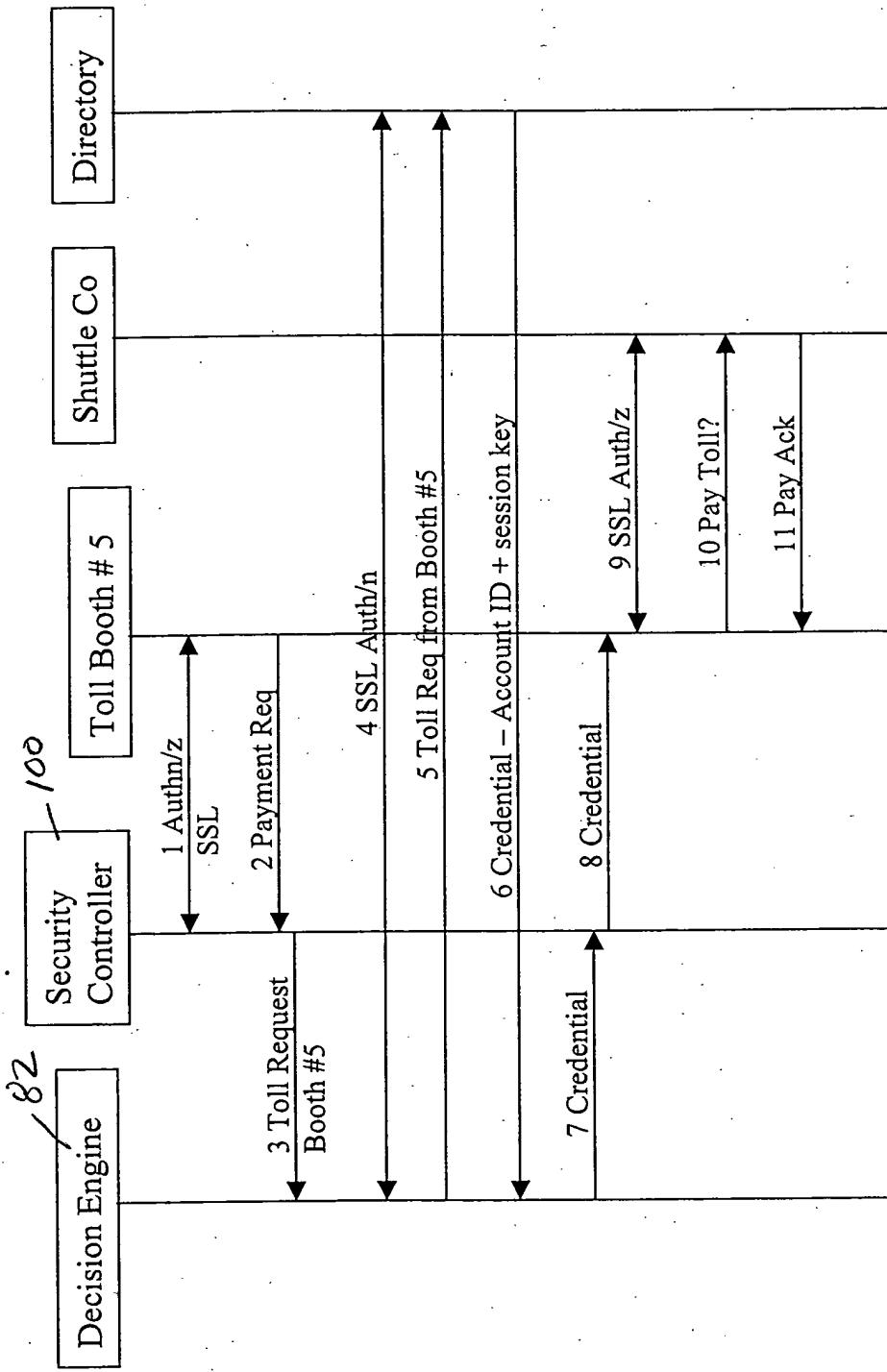


Fig. 5

## Anonymous, Secure Cab Fare Payment

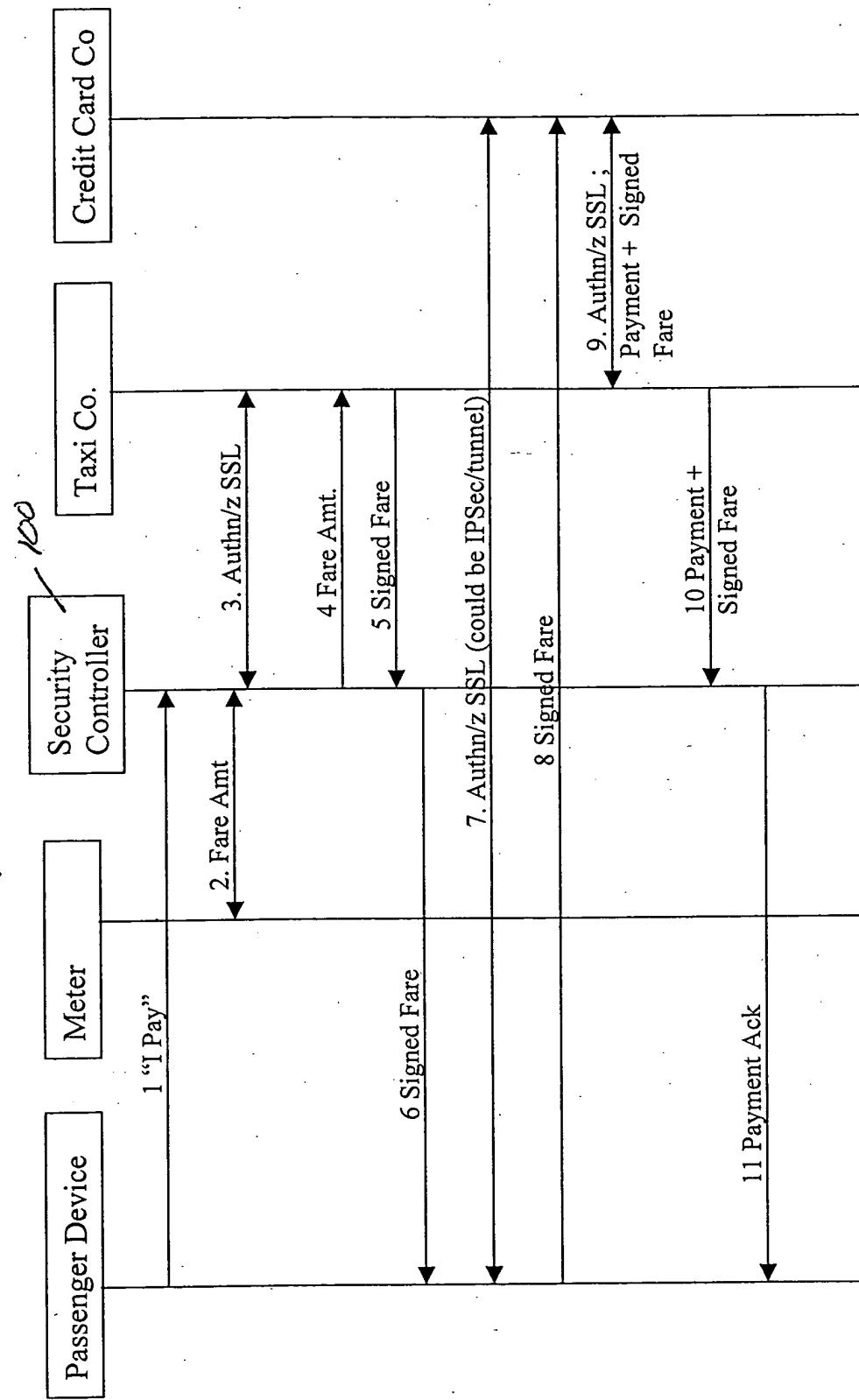


Fig. 6

## Secure Vehicle Location Access

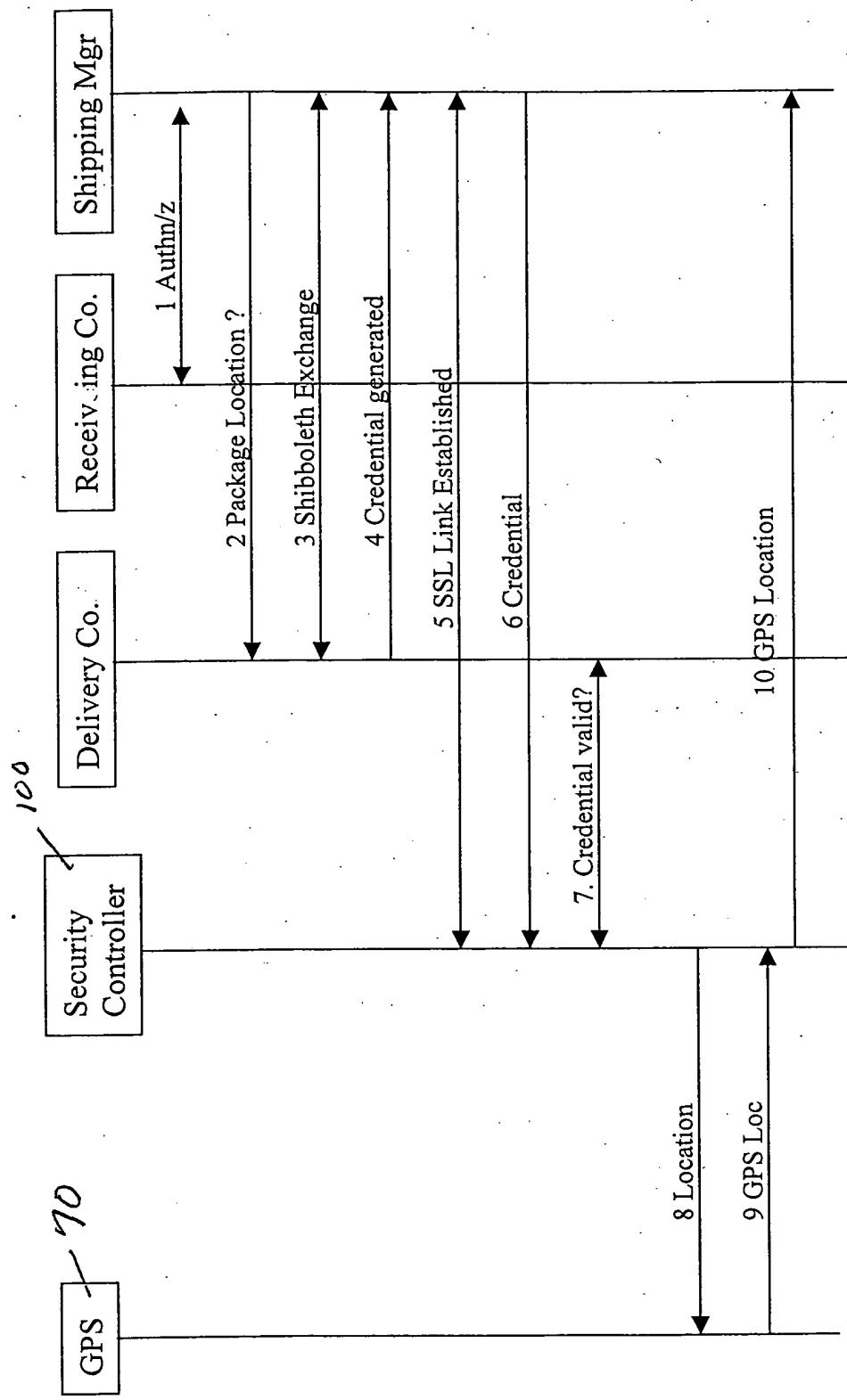


Fig. 7

## Secure Access to Vehicle Bus by Consumer Device

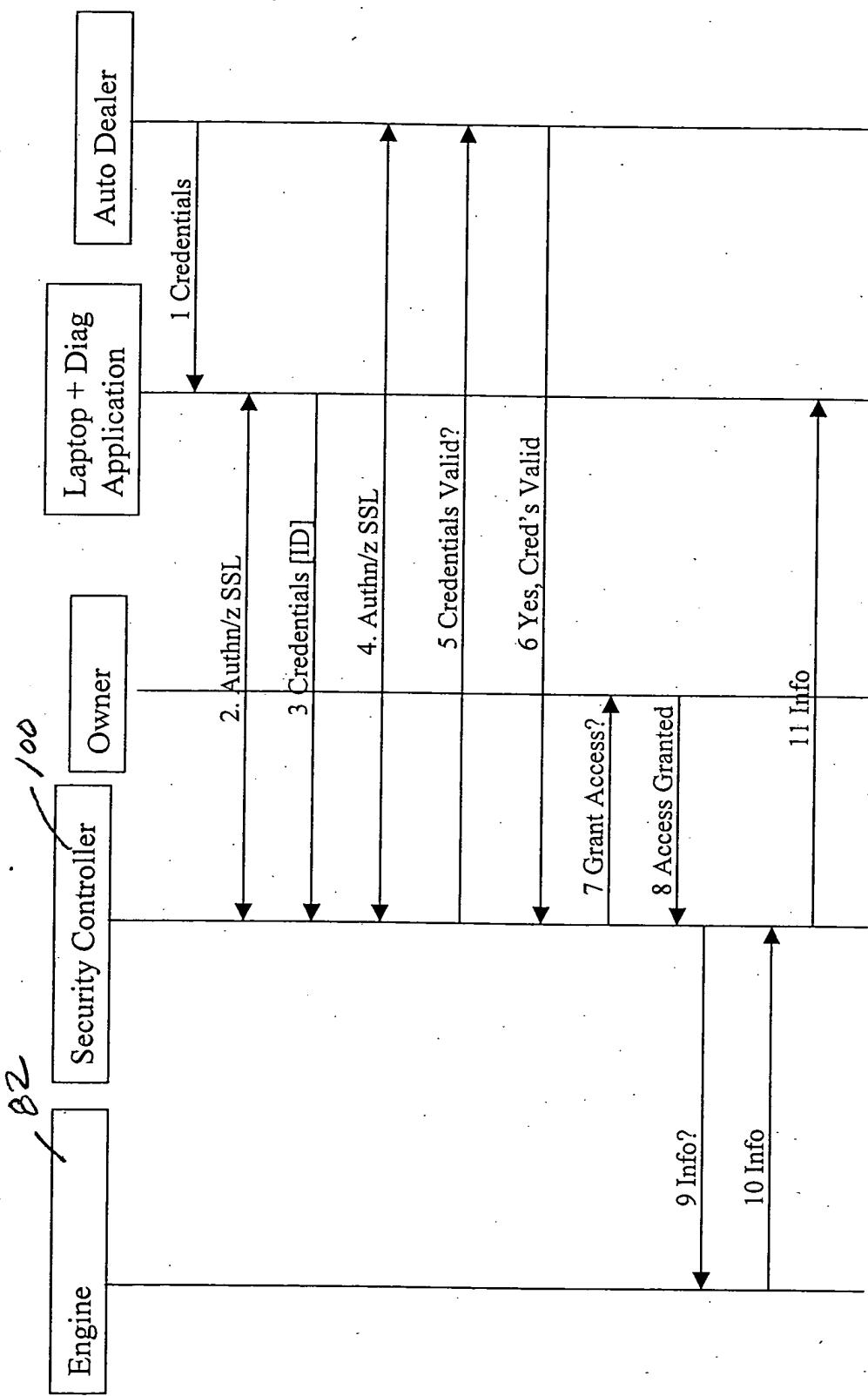


Fig. 8